

# SPPU-BE-COMP-CONTENT – KSKA Git

## CSDF UNIT 2 – PYQ Answers

➤ OCT – 2022

Q3

a) Explain in detail OS Security. [5]

**Operating System (OS) Security** refers to the measures and techniques used to **protect the operating system** from threats such as malware, unauthorized access, and data breaches. It ensures the **confidentiality, integrity, and availability** of system resources.

**Key Aspects of OS Security:**

### 1. User Authentication and Access Control

- Only authorized users can access the system through passwords, biometrics, or multi-factor authentication (MFA).
- Access control defines who can read, write, or execute files and resources.

### 2. Patch Management and Updates

- Regular updates and security patches fix known vulnerabilities in the OS.
- This helps prevent attackers from exploiting outdated software.

### 3. Malware and Virus Protection

- Use of antivirus software and intrusion detection systems (IDS) to monitor and remove threats.
- Firewalls are also used to filter incoming/outgoing network traffic.

### 4. File and Disk Encryption

- Encrypting sensitive files and storage prevents data theft even if the system is compromised.
- Tools like BitLocker (Windows) or LUKS (Linux) are commonly used.

### 5. System Logging and Auditing

- Keeps records of login attempts, file access, and system events.
- Helps in detecting suspicious activity and investigating breaches.

## SPPU-BE-COMP-CONTENT – KSKA Git

### b) What are different types of viruses and worms? How do they propagate? [5]

A virus is a malicious program that attaches itself to a host file and spreads when the file is executed. A worm is a self-replicating program that spreads across systems without needing to attach to a host file or user interaction.

Both are forms of malware designed to damage, steal, or corrupt data and resources.

#### Types of Viruses:

1. **File Infector Virus:**  
Attaches to executable files (.exe, .com) and runs when the file is opened. It spreads to other executable files on the system.
2. **Macro Virus:**  
Targets applications like MS Word or Excel by embedding malicious macros. It activates when the infected document is opened.
3. **Boot Sector Virus:**  
Infects the master boot record (MBR) of storage devices, making it hard to detect and remove. It runs before the OS even loads.
4. **Polymorphic Virus:**  
Changes its code every time it spreads, making it harder for antivirus software to detect. It is highly evasive and adaptive.

#### Types of Worms:

1. **Email Worm:**  
Spreads through email attachments or links, sending copies of itself to the victim's contact list automatically.
2. **Internet Worm:**  
Exploits network vulnerabilities to replicate across multiple machines without user action. Example: SQL Slammer, Conficker.
3. **Instant Messaging Worm:**  
Spreads via chat applications by sending malicious links or files to contacts in the friend list.

#### Propagation Methods:

- **Viruses propagate** by attaching themselves to legitimate files or software and activating when the file is executed by the user.
- **Worms propagate** through networks by exploiting security flaws, often requiring no user interaction.
- Both can spread via USB drives, email attachments, malicious websites, and shared networks.

### c) What do you mean by Intellectual Property? [5]

#### Definition:

**Intellectual Property (IP)** refers to creations of the mind—such as inventions, software, artistic works, designs, symbols, names, and business models—that are protected by law.

These laws give the creator **exclusive rights** to use, sell, or license their work and prevent unauthorized use by others.

In the digital age, IP is especially important due to easy duplication and distribution of digital content.

#### Types of Intellectual Property:

1. **Copyrights:**

Protects original creative works like books, music, software, movies, and paintings.  
Example: A software company holds copyright over its application code and UI design.  
Copyright protection exists automatically upon creation in a tangible form.

2. **Patents:**

Granted to inventors for new, useful, and non-obvious inventions.  
It gives exclusive rights to manufacture or sell the invention for a limited period (usually 20 years).  
Example: A patented mobile camera technology used in smartphones.

3. **Trademarks:**

Protects logos, symbols, words, or phrases used to represent a company or product.  
Example: The "Windows" name and the Microsoft logo are both trademarked.  
It helps prevent brand confusion and ensures uniqueness in the market.

4. **Trade Secrets:**

Includes confidential business information, formulas, practices, or processes.  
These are not registered but protected through confidentiality agreements.  
Example: Google's search algorithm or the KFC chicken recipe.

#### Relevance in Cybersecurity and Forensics:

- IP theft is a major **cybercrime**, especially in industries like software, media, and biotech.
- Cyber attackers may steal or leak IP for competitive, political, or financial gain.
- Protecting IP is essential to **preserve innovation, market position, and legal ownership**.

### Q4

#### a) Explain Internet Hacking and Different Approaches of Hacking. [5]

Internet hacking refers to the practice of gaining unauthorized access to computers, networks, or data over the internet. It is often done with malicious intent, such as stealing personal information, disrupting services, damaging data, or gaining financial benefit. Hackers exploit system vulnerabilities, software bugs, or user negligence to break into systems.

#### Different Approaches of Hacking

##### A. Phishing

- **Description:** Attackers impersonate legitimate entities (banks, companies) via fake emails or websites to steal sensitive data.
- **Example:** A fake "Bank Security Alert" email tricking users into entering login credentials.
- **Prevention:** User awareness, email filtering, multi-factor authentication (MFA).

##### B. Malware Attacks

- **Types:**
  - **Viruses:** Self-replicating programs that infect files.
  - **Trojans:** Disguised as legitimate software to gain access.
  - **Ransomware:** Encrypts files and demands payment for decryption.
- **Example:** WannaCry ransomware attack (2017).
- **Prevention:** Antivirus software, regular updates, backups.

##### C. Denial-of-Service (DoS/DDoS) Attacks

- **Description:** Overwhelming a server with fake traffic to crash it.
- **DDoS:** Distributed attack using multiple compromised devices (botnets).
- **Example:** Attack on Dyn DNS (2016) disrupting major websites.
- **Prevention:** Traffic filtering, cloud-based DDoS protection.

##### D. Man-in-the-Middle (MITM) Attacks

- **Description:** Hacker intercepts communication between two parties (e.g., Wi-Fi eavesdropping).
- **Example:** Stealing login credentials on public Wi-Fi.
- **Prevention:** Encryption (HTTPS, VPN), secure Wi-Fi protocols.

## SPPU-BE-COMP-CONTENT – KSKA Git

### E. SQL Injection

- **Description:** Injecting malicious SQL queries into web forms to manipulate databases.
- **Example:** Stealing user data from a vulnerable login page.
- **Prevention:** Input validation, parameterized queries.

### F. Zero-Day Exploits

- **Description:** Exploiting unknown vulnerabilities before developers can patch them.
- **Example:** Stuxnet worm targeting industrial systems.
- **Prevention:** Regular security patches, intrusion detection systems.

Internet hacking is a major cybersecurity threat that affects individuals, organizations, and governments. Understanding different hacking approaches is important for building **secure systems** and implementing **preventive measures** like firewalls, encryption, and regular updates.

### b) What are the different ways to gain access to your Computer System? [5]

Unauthorized access to a computer system is a key cybersecurity threat. Attackers use various methods to exploit **system vulnerabilities**, **user ignorance**, or **software flaws** to gain control of a target machine.

### Common Ways Attackers Gain Access to Computer Systems:

#### 1. Phishing Attacks

- Users are tricked into clicking fake links or entering sensitive credentials on fraudulent websites.
- These credentials are then used to access the system remotely.

#### 2. Malware Infections

- Malicious software like trojans, spyware, keyloggers, or ransomware is installed via email attachments or infected downloads.
- Malware can create backdoors or give attackers direct control over the system.

#### 3. Weak or Stolen Passwords

- Use of simple, reused, or default passwords makes systems vulnerable to brute-force or dictionary attacks.

## SPPU-BE-COMP-CONTENT – KSKA Git

- Attackers also steal passwords using keyloggers or data leaks.

### 4. Unpatched Software Vulnerabilities

- Operating systems or applications with outdated security patches can be exploited using known vulnerabilities.
- Attackers use tools to scan and exploit such weaknesses remotely.

### 5. Physical Access

- Direct access to a machine (e.g., unattended laptop) can allow an attacker to boot from external media or install keyloggers.
- Often exploited in shared or public environments.

### 6. Remote Desktop Exploits

- Misconfigured or unsecured Remote Desktop Protocol (RDP) connections can be exploited by attackers to gain remote access.

Attackers use a mix of **technical exploits** and **social engineering** to gain access to systems. Strong authentication, timely updates, and user awareness are key to preventing unauthorized access.

### c) Explain the significance of Firewall and VPN security technologies. [5]

**Firewall** and **VPN** are two essential security technologies used to protect systems and data from unauthorized access, cyberattacks, and privacy breaches. They play a crucial role in ensuring **network security** and **safe communication** over the internet.

#### 1. Firewall: Significance

A **firewall** is a network security device (or software) that monitors and controls **incoming and outgoing network traffic** based on predefined security rules.

##### Key Functions:

- Blocks unauthorized access to or from a private network.
- Filters traffic based on IP addresses, port numbers, and protocols.
- Prevents malware and hacker intrusion attempts.

## SPPU-BE-COMP-CONTENT – KSKA Git

### Example:

A firewall can block traffic from suspicious IP addresses trying to access your computer's open ports.

### 2. VPN (Virtual Private Network): Significance

A **VPN** creates a **secure, encrypted tunnel** over the internet between the user's device and the destination network.

#### Key Functions:

- Encrypts internet traffic, protecting data from eavesdropping.
- Hides user IP address, enhancing privacy.
- Enables secure access to remote networks (e.g., for remote workers).

### Example:

When using public Wi-Fi in a café, a VPN prevents hackers from intercepting sensitive data like passwords or banking info.

### Comparison Table

Feature	Firewall	VPN
Primary Role	Blocks unauthorized traffic	Encrypts & anonymizes internet traffic
Protection	Network-level security	Data-level security
Best Used For	Preventing intrusions	Secure remote access & privacy

➤ SEP 2023

Q3

#### a) What is meant by Internet Hacking & Cracking? Explain Types of Cracking. [7]

**Internet hacking** is the act of **gaining unauthorized access** to computers, networks, or data over the internet. It involves exploiting system vulnerabilities to:

- Steal sensitive information
- Alter or destroy data

## SPPU-BE-COMP-CONTENT – KSKA Git

- Disrupt services or gain control of systems  
Hackers may use malware, phishing, or network attacks to achieve this.

### Cracking

**Cracking** is a subset of hacking, focused on **bypassing or removing security mechanisms** from software or systems. Unlike ethical hacking, cracking is usually performed with malicious or illegal intent — such as bypassing license verification, stealing passwords, or breaking into encrypted data.

### 3. Types of Cracking:

#### i. Password Cracking

- Involves retrieving or guessing user passwords.
- Methods include brute force attacks, dictionary attacks, and social engineering.
- Used to access user accounts or secured systems.

#### ii. Software Cracking

- Disabling software copy protection or license enforcement.
- Enables illegal use of premium or paid software without purchase.
- Common in pirated applications.

#### iii. Network Cracking

- Breaking into secure wireless networks (e.g., Wi-Fi) by bypassing encryption like WPA/WPA2.
- Attackers may capture traffic, steal credentials, or inject malware.

#### iv. Email Cracking

- Gaining access to someone's email account by guessing or stealing their login credentials.
- Often used in identity theft, phishing, or blackmail.

#### v. Serial Key Cracking / Keygens

- Generating fake product keys using software tools.
- Used to unlock paid software illegally without genuine purchase.

---

While **hacking** often involves broader system-level attacks, **cracking** is specifically aimed at **breaking protections** to gain unauthorized use of resources or data. Both are considered illegal when done without permission and pose serious threats to cybersecurity.



## SPPU-BE-COMP-CONTENT – KSKA Git

### b) What are the different computer intrusions? Differentiate between Virus and Worms. [8]

**Computer intrusion** refers to any unauthorized activity that compromises the confidentiality, integrity, or availability of computer systems or data. It typically involves breaching system defenses to **steal, damage, or alter data** or disrupt operations.

#### Types of Computer Intrusion:

##### i. Malware Intrusion

- Includes viruses, worms, trojans, spyware, ransomware, etc.
- Injects harmful code into the system to disrupt or control operations.

##### ii. Phishing Attacks

- Trick users into revealing sensitive information through fake websites or emails.

##### iii. Brute Force Attacks

- Repeatedly trying different passwords or encryption keys to gain unauthorized access.

##### iv. Denial of Service (DoS)

- Overwhelms systems or networks with traffic, making services unavailable to legitimate users.

##### v. Rootkits

- Malicious tools that hide their presence while providing privileged access to the attacker.

##### vi. Keylogging

- Secretly records user keystrokes to capture login credentials or sensitive information.

#### Difference Between Virus and Worm:

Aspect	Virus	Worm
Definition	A virus is a malicious program that <b>attaches itself to a host file</b> or program.	A worm is a <b>self-replicating</b> program that spreads without a host.
Spread Method	Requires <b>user action</b> (like opening a file) to spread.	Spreads <b>automatically</b> over networks or the internet.
Dependency	Needs a host program or file to execute.	Independent; does not need a host file.
Damage	Corrupts files, modifies programs, and slows system performance.	Consumes bandwidth, slows networks, and may drop

## SPPU-BE-COMP-CONTENT – KSKA Git

Aspect	Virus	Worm
		payloads.
Example	Melissa virus, ILOVEYOU	SQL Slammer, Conficker worm

Computer intrusions can take many forms — from malware infections to network attacks — all posing serious threats to systems and data. **Viruses and worms** are both types of malware, but they differ significantly in their method of propagation and system impact. Understanding these differences helps in implementing proper cybersecurity defenses.

Q4)

a) Explain backups, archival storage & disposal of data in data security. [7]

Data security not only involves preventing unauthorized access but also includes **proper management of data throughout its lifecycle** — including **backups**, **archival**, and **secure disposal**. These practices ensure data integrity, availability, compliance, and protection against loss or misuse.

### Backups:

A **backup** is a **copy of data** stored separately from the original source, created to recover information in case of data loss due to accidental deletion, system failure, malware attacks, or natural disasters.

#### Types of Backups:

- **Full Backup:** Complete copy of all data.
- **Incremental Backup:** Backs up only the changes made since the last backup.
- **Differential Backup:** Backs up changes since the last full backup.

#### Importance:

- Enables **disaster recovery**.
- Ensures **business continuity**.
- Helps in **restoring accidentally deleted files** or systems affected by ransomware.

### Archival Storage:

**Archival storage** refers to the long-term storage of data that is **rarely accessed** but must be **retained for legal, regulatory, or historical purposes**.

#### Characteristics:

- Stored in compressed, read-only formats.

## SPPU-BE-COMP-CONTENT – KSKA Git

- Slower retrieval time compared to active storage.
- Cost-effective for long-term data retention.

### Examples:

- Financial records, old emails, logs, medical records.
- Stored in cloud-based archival systems (e.g., AWS Glacier, Google Cloud Archive).

### Disposal of Data:

**Data disposal** is the process of **securely deleting or destroying data** that is no longer needed, to prevent unauthorized recovery or misuse.

#### Methods:

- **Data wiping:** Overwriting data with random values.
- **Degaussing:** Disrupting magnetic fields of storage media.
- **Physical destruction:** Shredding or crushing hard drives and storage devices.

#### Importance:

- Ensures **compliance with data protection laws** (e.g., GDPR).
- Prevents **data leaks and identity theft**.
- Frees up storage and reduces risk of outdated data exposure.

### b) Describe firewall security technology with neat diagram. [8]

A **firewall** is a security device (hardware, software, or both) that monitors and controls incoming and outgoing network traffic based on pre-defined security rules. It acts as a barrier between a **secure internal network (LAN)** and **untrusted external networks (like the Internet)**.

The primary purpose of a firewall is to **permit legitimate traffic** and **block suspicious or unauthorized access** attempts to ensure network security.

#### Working of Firewall:

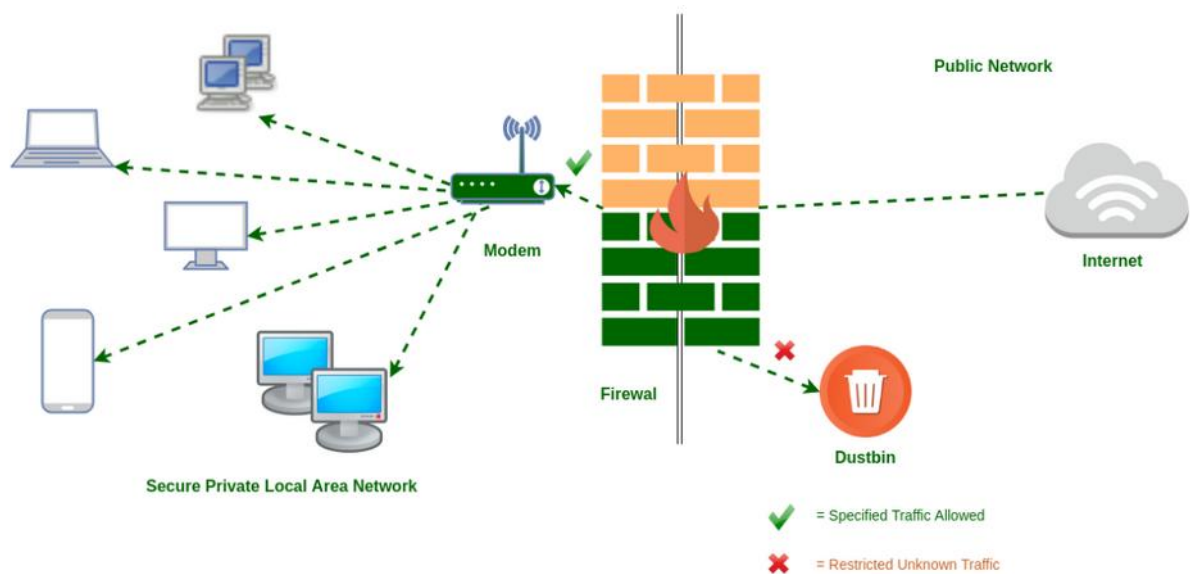
As shown in the diagram:

- Devices like laptops, phones, desktops, and other computers are connected to the **Secure Private Local Area Network (LAN)** through a **modem**.
- All data traffic passes through the **firewall**, which checks whether the traffic complies with the defined security rules.
- **Authorized traffic** is forwarded to the **Internet (Public Network)**.
- **Unknown, harmful, or restricted traffic** is blocked and **discarded (sent to dustbin)**.

## SPPU-BE-COMP-CONTENT – KSKA Git

This selective filtration helps in:

- Preventing malware and hacking attempts
- Controlling bandwidth usage
- Blocking access to inappropriate websites or IPs
- Ensuring only safe communication between internal and external networks



➤ SEP 2024

Q3)

a) What is Unauthorized Access? What are the common causes of Unauthorized Access? [5]

**Unauthorized Access:**

Unauthorized access refers to **gaining access to a system, network, or data without permission or proper authorization**. It is a **serious security violation** that can lead to data breaches, loss of privacy, or manipulation of critical information. This type of access is often performed by hackers, malicious insiders, or due to weak system protections.

**Common Causes of Unauthorized Access:**

1. **Weak Passwords:**

- Use of simple, easily guessable, or reused passwords makes it easy for attackers to gain access through brute force or dictionary attacks.

## SPPU-BE-COMP-CONTENT – KSKA Git

### 2. Phishing Attacks:

- Attackers trick users into revealing their login credentials through fake emails or websites that appear legitimate.

### 3. Malware and Spyware:

- Malicious software can log keystrokes or steal credentials, giving attackers direct access to systems or networks.

### 4. Unpatched Software or System Vulnerabilities:

- Outdated software or operating systems may have known security loopholes that attackers exploit.

### 5. Poor Access Control Policies:

- Granting unnecessary or excessive access rights to users or devices can expose sensitive data to unauthorized parties.

Unauthorized access is a critical cybersecurity issue, and organizations must implement strong **authentication, encryption, and monitoring mechanisms** to prevent it.

## b) How to Prevent Unauthorized Computer Access? [5]

Preventing unauthorized access is essential to protect computer systems, networks, and sensitive data. Below are **effective methods** to reduce the risk of unauthorized access:

### 1. Use Strong Passwords and Multi-Factor Authentication (MFA):

- Enforce complex password policies (mix of letters, numbers, symbols).
- Implement MFA using OTPs, biometric verification, or authentication apps for added security.

### 2. Install Antivirus and Anti-Malware Software:

- Use updated security software to detect and block malware, trojans, keyloggers, and spyware.
- Regularly scan systems for threats and remove malicious files.

### 3. Keep Systems and Software Updated:

- Regularly patch operating systems and applications to fix known security vulnerabilities.
- Enable automatic updates where possible to stay protected.

## SPPU-BE-COMP-CONTENT – KSKA Git

### 4. Use Firewalls and Network Security Tools:

- Configure firewalls to monitor and control incoming/outgoing traffic.
- Set up intrusion detection/prevention systems (IDS/IPS) to detect abnormal activities.

### 5. Restrict Physical and Logical Access:

- Use user access control, permissions, and role-based access.
- Limit access to sensitive systems and areas only to authorized personnel.

By following these practices, organizations and individuals can significantly reduce the risk of unauthorized access, ensuring the **confidentiality, integrity, and availability** of their systems and data.

### c) What is Application Security? State its Different Types. [5]

#### Application Security:

**Application security** refers to the **measures, tools, and practices** used to **protect software applications** from threats and vulnerabilities throughout their lifecycle — from development to deployment and maintenance.

It ensures that applications function correctly even under malicious attacks, thereby preserving **data confidentiality, integrity, and availability**.

#### Types of Application Security:

##### 1. Authentication Security:

- Verifies the identity of users before allowing access.
- Methods include passwords, biometric scans, OTPs, or multi-factor authentication.

##### 2. Authorization Security:

- Ensures that authenticated users can only access the data or functions they are allowed to.
- Implements role-based access controls (RBAC).

##### 3. Data Encryption:

- Converts sensitive data into unreadable form to protect it during transmission and storage.
- Common algorithms include AES, RSA, and SSL/TLS protocols.

## SPPU-BE-COMP-CONTENT – KSKA Git

### 4. **Input Validation:**

- Ensures user inputs are sanitized and checked before processing to prevent attacks like SQL injection or cross-site scripting (XSS).

### 5. **Session Management Security:**

- Protects user sessions from hijacking or unauthorized reuse using secure tokens, timeout mechanisms, and HTTPS.

Application security is crucial for defending against modern cyber threats and should be integrated during the **software development lifecycle (SDLC)** to build secure and robust applications.

**Q4)**

### **a) How Email Hacking Takes Place? [5 Marks]**

**Email hacking** refers to unauthorized access to a person's or organization's email account to steal sensitive information, send spam, or launch further attacks. It is a **common cybercrime technique** used for identity theft, phishing, and spreading malware.

#### **Methods of Email Hacking:**

##### 1. **Phishing Attacks:**

- Hackers send fake emails pretending to be from legitimate sources (like banks or government sites).
- These emails trick users into clicking malicious links or entering their login credentials on fake websites.

##### 2. **Password Guessing & Brute Force Attacks:**

- Weak or commonly used passwords can be guessed or cracked using automated tools that try millions of combinations.

##### 3. **Keylogging Malware:**

- Malicious software secretly records keystrokes on the victim's device.
- Login details typed while accessing email accounts are captured and sent to the attacker.

##### 4. **Public Wi-Fi Exploits:**

- Hackers on unsecured Wi-Fi networks can intercept data being transmitted, including email login sessions if not encrypted.

##### 5. **Data Breaches & Credential Leaks:**

- Hackers use previously leaked email-password combinations (from data breaches) to access accounts that reuse passwords.

## SPPU-BE-COMP-CONTENT – KSKA Git

Email hacking can lead to **data theft, blackmail, financial loss, or further cyberattacks**, making it essential to use strong passwords, enable multi-factor authentication, and avoid clicking on suspicious email links.

### b) What is Hardware Protection? What are the Different Types of Hardware Protection? [5]

**Hardware Protection:** Hardware protection refers to the **techniques and mechanisms used to safeguard physical computing devices** (like CPUs, memory units, storage, and peripherals) from unauthorized access, damage, or misuse. It ensures the **security, reliability, and proper functioning** of hardware components in a computer system.

#### Different Types of Hardware Protection:

1. **Memory Protection:**
  - Prevents one process from accessing the memory space of another.
  - Ensures data isolation and prevents malicious code execution.
2. **I/O Protection:**
  - Restricts unauthorized programs from directly accessing input/output devices.
  - Uses privileged instructions to control hardware communication securely.
3. **CPU Protection:**
  - Uses timers and processor modes (user mode vs kernel mode) to avoid CPU misuse by a single process.
  - Helps prevent infinite loops and overloads.
4. **Access Control Mechanisms:**
  - Physical methods like biometric locks, smart cards, or RFID-based authentication to restrict physical access to hardware.
5. **Power Supply and Surge Protection:**
  - Protects hardware from electrical damage using UPS systems and surge protectors.
  - Ensures safe shutdown during power failures.

Hardware protection is essential to prevent physical tampering, unauthorized use, and hardware-level attacks that could compromise the entire computing environment.

### c) What are the Types of Program Threats and System Threats? [5]

**1. Program Threats:** Program threats are malicious code segments embedded in legitimate programs that can harm the system when executed.

#### Types of Program Threats:



## SPPU-BE-COMP-CONTENT – KSKA Git

- **Trojan Horse:**
  - A malicious program disguised as a useful or harmless one.
  - Performs harmful actions like deleting files or installing spyware when executed.
- **Trapdoor (Backdoor):**
  - Hidden entry point into a program that allows unauthorized access without normal authentication.
  - Often used by developers or attackers to bypass security.
- **Logic Bomb:**
  - A code that triggers malicious activity when specific conditions are met (e.g., a date or event).
  - Can delete data or crash systems upon activation.
- **Virus:**
  - A self-replicating program that spreads by attaching itself to files or programs.
  - Can corrupt data, slow down systems, or crash software.

### 2. System Threats:

System threats aim to disrupt the functioning of entire systems or networks, often from external sources.

#### Types of System Threats:

- **Worms:**
  - Self-replicating programs that spread through networks without attaching to files.
  - Can cause network congestion and resource overuse.
- **Denial of Service (DoS) Attacks:**
  - Flooding a server or network with excessive requests to make it unavailable to legitimate users.
- **Port Scanning:**
  - Scanning a system's ports to find vulnerabilities for exploitation.

Both program and system threats pose significant risks to the **confidentiality, integrity, and availability** of data and resources, making proper security mechanisms essential.

**Disclaimer -**

**"Check/Verify Answer – Read at Your Own Risk"**